

Marlene H. Dortch, Secretary Federal Communications Commission The Portals 445 12th Street, SW Washington, DC 20554

Re: RCN Telecom Services, Inc.

RCN Telecom Services of Illinois, LLC RCN Telecom Services of Philadelphia, Inc.

RCN-BecoCom, LLC

Starpower Communications, LLC

Certification of CPNI Filing (2-6-06)

EB Docket No. 06-36

EB-06-TC-060

Dear Ms. Dortch:

Pursuant to the Public Notice issued by the Enforcement Bureau on January 30, 2006¹ and the Commission rules concerning telecommunications carriers protection of the privacy of customer proprietary network information ("CPNI"),² RCN Telecom Services, Inc.; RCN Telecom Services of Illinois, LLC; RCN Telecom Services of Philadelphia, Inc.; RCN-BecoCom, LLC; and Starpower Communications, LLC (collectively, "RCN") file the attached Compliance Statement and Certificate. RCN recognizes its obligation to protect the privacy of customer information and has put into practice various operational procedures to assure that, consistent with the Commission's rules, its customers' CPNI is protected from unauthorized and illegal use, access and disclosure.

Respectfully submitted,

Timothy J. Dunne

Executive Vice President

Chief Technology Officer

cc: Bryon McKoy via e-mail: byron.mccoy@fcc.gov Best Copy and Printing via e-mail: fcc@bcpiweb.com

Enforcement Bureau Directs All Telecommunications Carriers to Submit CPNI Compliance Certifications, Public Notice, DA 06-223 (rel. Jan. 30, 2006) ("Public Notice").

² 47 C.F.R. § 64.2001, et seq.

CPNI COMPLIANCE CERTIFICATE & STATEMENT

I hereby certify that I am an officer of RCN Telecom Services, Inc.; RCN Telecom Services of Illinois, LLC; RCN Telecom Services of Philadelphia, Inc.; RCN-BecoCom, LLC; and Starpower Communications, LLC (collectively, "RCN"), and am authorized to execute this Certificate as agent for each of these entities. Based upon my personal knowledge, I certify that the following statement describes the processes and procedures adopted by RCN to protect the privacy of its customers' CPNI pursuant to the Federal Communications Commission's CPNI rules, 47 CFR §§ 64.2001 – 64.2009.

RCN has adopted a Code of Business Conduct, which must be reviewed and signed by all employees as part of the hiring process. Among other things, the Code of Business Conduct emphasizes the confidentiality of all customer account information. All managers are required to certify annually that they are in compliance with the Code and have communicated these policies to their subordinates. RCN maintains a Compliance Hotline that any employee may use to report violations of company policies. Any violations of the Code of Business Conduct may result in disciplinary action up to and including dismissal from employment.

Those employees who have access to customer account records (including marketing, telesales representatives, and customer service representatives) are required to undergo a training program before beginning their duties. The training course includes a review of the Code of Business Conduct and account security procedures. Customer service representatives are specifically trained to verify the identity of the customer before discussing any account information, including obtaining a PIN number from those customers who have established one.

RCN does not share, sell, lease or otherwise permit access to individually identifiable CPNI to any unaffiliated third parties, except as expressly directed by a customer in writing. RCN may permit access to CPNI by independent contractors and/or agents for use in providing and/or marketing RCN services, only after such contractor or agent has executed a confidentiality agreement. RCN also maintains a customer privacy policy, which is posted on its website, which prohibits the sale or lease of any customer information for purposes other than the provision or marketing of RCN services.

As permitted by the CPNI rules, RCN may use, disclose, and permit access to CPNI (1) to bill and collect for services rendered; (2) to protect rights or property of RCN, other users or other carriers from unlawful use; (3) to provide any inbound telemarketing or administrative services for the duration of a call; (4) for the purpose of providing carrier premises equipment ("CPE") and protocol conversion; and (5) in order to provision inside wiring, maintenance and repair services.

The RCN billing system includes a privacy "flag" that can be activated on any account upon customer request (opt-out). Once this flag is enabled, it is not disabled for any reason other than a customer's instructions. Customers whose accounts are flagged do not receive any marketing-related telephone or mail contacts from RCN.

RCN has established a procedure for supervisory review of all outbound marketing activities. All marketing campaigns must be approved in writing by the general manager of the region, the Chief Financial Officer and the Chief Technology Officer of RCN. Records of these approvals are retained by RCN's product management group.

Respectfully submitted,

Timothy J. Dunne

Executive Vice President Chief Technology Officer

February 6, 2006